Amendments to the Claims:

1. (Currently Amended) A method for securing transactions using electronic deposits (purses), comprising:

~~combining~~ configuring, in an electronic deposit (purse), a grey lock mark, which identifies the state of the last transaction of the electronic deposit (purse); after setting the grey lock mark, all operations to the electronic deposit (purse) except resetting the grey lock mark being invalidated ~~with an electronic deposit (purse) of an IC card~~;

setting, while starting a transaction using the electronic deposit (purse), the grey lock mark and ~~a grey lock mark on the IC card to lock grey the IC card while simultaneously~~ recording parameters of the transaction as a locking card source in the electronic deposit (purse) ~~a first locking card source by the IC card~~; and

~~merging a debiting operation and a unlocking grey operation into a one step operation on the IC card; and~~

validating the recorded locking card source before debiting money from the electronic deposit (purse), and if the recorded parameters are validated, debiting money from the electronic deposit (purse) and resetting the grey lock mark simultaneously ~~to unlock grey the IC card automatically after successfully completing the debiting operation~~.

2. (Currently Amended) The method according to claim 1, further comprising:

storing an encryption key in a host computer of the distributor who distributes the electronic deposit (purse), in order to debit supplementary money from the electronic deposit (purse) and to reset the grey lock mark compulsorily in the electronic deposit (purse), which is being set the grey lock mark, ~~of implementing a debiting operation and implementing a mandatory unlocking grey operation in a computer to make a supplementary debit and implementing a mandatory unlocking grey operation for a locked grey IC card~~ on an on-line card terminal by an ~~with~~ on-line mode.

3. (Currently Amended) The method according to claim 1, wherein the procedure of securing transactions using electronic deposits (purse) comprises ~~comprising~~:

inserting the electronic deposit (purse) into a transaction ~~IC card to a card~~ terminal;

authenticating mutually by ~~both~~ the electronic deposit (purse) ~~IC card and the card~~ and the terminal ~~mutually~~;

~~locking~~ setting the grey mark in the ~~IC card~~ electronic deposit (purse) by the ~~card~~ terminal;

performing ~~initiating~~ a consumption; and

after the consumption is complete, debiting appropriate money from [[an]] the electronic deposit (purse) ~~on the IC card and unlocking~~ resetting the grey mark simultaneously ~~the IC card~~ by the ~~card~~ terminal.

4. (Currently Amended) The method according to claim 3, wherein the step of ~~locking~~ setting the grey ~~the IC card~~ lock mark comprises:

generating ~~creating~~ a first ~~authentication~~ locking code by the electronic deposit (purse) ~~IC card~~ according to the ~~first~~ locking card source and ~~transferring~~ transmitting simultaneously the ~~necessary parameters for creating the first~~ locking card source to the ~~card~~ transaction terminal using the electronic deposit (purse) ~~simultaneously~~;

generating ~~creating~~ a second locking card code ~~source~~ by the ~~card~~ terminal ~~using~~ in the same ~~mechanism~~ way as the electronic deposit (purse) ~~IC card,~~ and ~~with the second locking card source creating~~ generating a ~~second~~ first authentication code according to the second locking code and sending the ~~second~~ first authentication code to the electronic deposit (purse) ~~IC card by the card terminal~~;

generating a second authentication code by the electronic deposit (purse) according to the first locking code in the same was as the terminal;

determining ~~by the IC card~~ whether the received first authentication code and the generated second authentication code are identical, and if yes ~~they are~~, ~~locking~~ setting the grey lock mark ~~the IC card and sending back a grey lock characterized code, created with the first locking card source and corresponding data, to the card terminal~~; and

wherein ~~said~~ the step of debiting money from [[an]] the electronic deposit (purse) ~~on the IC card~~ and resetting the ~~unlocking~~ grey lock mark ~~the IC card by the card terminal~~ simultaneously, comprises:

generating ~~creating~~ a third authentication code ~~by the card terminal~~ according to the second lock code and ~~locking card source and necessary~~ parameters for debiting money from the electronic deposit (purse) by the terminal, and sending the generated third authentication code and the ~~corresponding~~ parameters ~~together~~ to the electronic deposit (purse) ~~IC card~~;

generating ~~creating~~ a fourth authentication code according to ~~by the IC card with~~ the first ~~locking card source~~ lock code and the ~~corresponding~~ received parameters by the electronic deposit (purse) ~~using same mechanism~~; and

determining ~~by the IC card~~ whether the received third authentication code and the generated fourth authentication code are identical, and if yes ~~they are~~, debiting money from [[an]] the electronic deposit (purse) ~~on the IC card~~ and resetting the grey lock mark simultaneously after debiting successfully.

5. (Currently Amended) The method according to claim 4, wherein the step of validating the recorded locking card source comprises ~~further comprising~~:

generating a fifth authentication code according to the first locking code by the electronic deposit (purse) and sending the fifth authentication code to the terminal;

generating a sixth authentication code according to the second locking code by the terminal and determining whether the received fifth authentication code and the generated sixth authentication code are identical, if yes, it means that the recorded locking card source is validated, otherwise, the recorded locking card source is invalidated; and

if the transaction using the electronic deposits (purses) is incomplete, the method further comprising:

storing the ~~third~~ sixth authentication code ~~needed for debiting, the amount of money of an escape card and the grey lock characterized code~~ and parameters for debiting money from the electronic deposits (purses) together as part of a grey record information by the terminal, and

sending the grey record information to the host computer of the distributor who distributes the electronic deposit (purse) ~~a central computer by the card terminal~~; and

if the electronic deposit (purse) is used in any terminal that stores the grey record information, before validating the recorded locking card source, the method further comprising:

regenerating the fifth authentication code according to the recorded locking card source by the electronic deposit (purse) and send the fifth authentication code to the terminal.

~~for an IC card with an incomplete ending transaction and without debiting and unlocking the last time the IC card was used, authenticating the grey lock characterized code by the card terminal the next time the IC card is used, which terminal has stored said grey record, to confirm that the first locking card source of the IC card is same as the second locking card source for calculating the third authentication code in said grey record; and after confirmation, executing the debit and unlocking grey operation.~~

6. (Currently Amended) The method according to claim 1, wherein ~~said first locking card source is~~ the step of generating a first locking code according to the locking card source comprises:

generating a procedure encryption key (SESPK), correlating to at least a pseudo random number (ICC) created temporarily, in the electronic deposit (purse) ~~by the IC card~~.

7. (Currently Amended) The method according to claim 6, wherein ~~said~~ the equation of generating a procedure encryption key (SESPK) comprises:

the procedure encryption key (SESPK) = 3DES (DPK, DATA), where DPK is a consumption encryption key of the electronic deposit (purse~~), obtained from a consumption main encryption key (MPK) based on dispersing an application sequence number of the IC card~~; and DATA is a specific parameter including a ~~temporarily created~~ pseudo random number (ICC) temporarily created by the electronic deposit (purse) ~~of said IC card~~, a transaction sequence number of the electronic deposit (purse) (CTC), and the last two bytes of the ~~card~~ terminal transaction sequence number (TTC).

8. (Currently Amended) The method according to claim 6, wherein the step of setting the grey lock mark comprises:

locking grey the IC card comprises:

sending a ~~card~~ terminal transaction sequence number (TTC) ~~from the card terminal~~ to the electronic deposit (purse) by the terminal ~~IC card~~;

getting a pseudo random number (ICC) and an electronic deposit (purse) transaction sequence number (CTC) by the electronic deposit (purse) ~~of the IC card~~;

generating ~~creating~~ a first procedure encryption key (SESPK) ~~by the IC card~~ and recording the parameters of this generating ~~creating~~ step and also generating ~~creating~~ and recording a ~~grey lock characterized~~ sixth authentication code of this time ~~at the same time~~;

sending the pseudo random number (ICC) and the electronic deposit (purse) transaction sequence number (CTC) from the electronic deposit (purse) ~~IC card~~ to the ~~card~~ terminal, which ~~terminal~~ has stored a consumption main encryption key (MPK) in its security authentication module (PSAM);

deriving the electronic deposit (purse) DPK ~~on the IC card with an application sequence number of the IC card~~ by the security authentication module (PSAM); and

generating ~~creating~~ a second procedure encryption key (SESPK) by the ~~card~~ terminal using the pseudo random number (ICC), the electronic deposit (purse) transaction sequence number (CTC), and the ~~card~~ terminal transaction sequence number (TTC) in ~~using~~ the same ~~mechanism~~ way as the electronic deposit (purse) ~~IC card~~; and

wherein ~~said~~ the step of debiting money from the electronic deposit (purse) and resetting the grey lock mark simultaneously ~~step~~ comprises:

generating the third ~~calculating a first~~ authentication code by the ~~card~~ terminal according to ~~with~~ the second procedure encryption key (SESPK), and at least the debit amount, operation date and time, and sending the ~~first~~ third authentication code, the second procedure encryption key (SESPK), and at least the debit amount, operation date and time to the electronic deposit (purse) ~~IC card~~;

generating the fourth ~~calculating a second~~ authentication code by the electronic deposit (purse) according to ~~IC card with~~ the first procedure encryption key (SESPK), using the same data and algorithm as the terminal;

determining by the ~~IC card~~ electronic deposit (purse) whether the ~~first~~ third authentication code and the ~~second~~ fourth authentication code are identical, and if yes ~~they are, then~~ debiting money and resetting the grey lock mark ~~unlocking~~, and otherwise ~~if they are not, then~~ incrementing an internal error counter and returning an error code without debiting money from the electronic deposit (purse) and resetting the grey lock mark simultaneously ~~unlocking~~; and

locking the electronic deposit (purse) ~~IC card application~~ internally to prevent misuse, when the internal error counter reaches a predetermined number.

9. (Currently Amended) The method according to claim 1, wherein the step of setting ~~combining~~ a grey lock mark ~~with an electronic deposit~~ comprises creating a refueling electronic deposit.

10. (Currently Amended) The method according to claim 9, wherein said refueling electronic deposit ~~further~~ includes the functions of refueling transaction, local ~~unlocking grey~~ transaction for resetting the grey lock mark and on-line ~~unlocking grey~~ transaction for resetting the grey lock mark.

11. (Currently Amended) The method according to claim 9, wherein said refueling electronic deposit further includes the states of pre-refueling, grey lock and unlocked grey.

12. (Currently Amended) The method according to claim 9, wherein said refueling electronic deposit further ~~includes~~ comprises the commands of INITIALIZE FOR REFUEL, LOCK FOR REFUEL, DEBIT FOR REFUEL, INITIALIZE FOR UNLOCK, DEBIT FOR UNLOCK and GET GREY STATUS, wherein the INITIALIZE FOR REFUEL command is used for refueling consumption transaction initialization, the LOCK FOR REFUEL command is used for making grey lock to refueling electronic deposit (purse), the DEBIT FOR REFUEL command is used for local refueling consumption and unlocking grey simultaneously, the

INITIALIZE FOR UNLOCK command is used for on-line unlocking and consumption transaction initialization, the DEBIT FOR UNLOCK command is used for on-line unlocking grey transaction and supplementary debiting refueling consumption simultaneously, and the GET GREY STATUS command is used for reading grey lock state and launching local unlocking grey transaction.